



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **08251156 A**(43) Date of publication of application: **27.09.96**

(51) Int. Cl. **H04L 9/06**
H04L 9/14
G06F 13/00
G09C 1/00
H04L 12/54
H04L 12/58

(21) Application number: **07052252**(22) Date of filing: **13.03.95**(71) Applicant: **HITACHI LTD**

(72) Inventor: **NISHIOKA GENJI**
MIYAZAKI SATOSHI

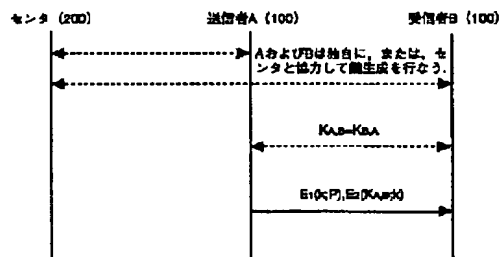
(54) METHOD AND SYSTEM FOR CIPHERING ELECTRONIC MAIL**(57) Abstract:**

PURPOSE: To provide an electronic mail ciphering method which can be used with a normal mail together without specifying the mail system and the kind of device, reduces calculation processing and the burden of memory for attaining a security function for persons both transmitting electronic mail and receiving it, and is provided with high safety against tapping and a unauthorized persons who set up to be authorized without any need to worry about the coincidence of users' keys.

CONSTITUTION: Each user of a communication network prepares key information of each and opens only an open key. Next, the transmitter A and the receiver B of the electronic mail share master keys KA, B and KB, A from his own secret key and the open key of the opposite side and the transmitter ciphers the body sentences P of the mail by a data ciphering key (k) through the use of the secret key cipher. Then the data ciphering key is ciphered by the master key. Then, they are sent to the receiver and the receiver deciphers the data ciphering key (k) through the use of the master key KB, A and

deciphers the mail body sentence P from the data ciphering key (k) in addition.

COPYRIGHT: (C)1996,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-251156

(43) 公開日 平成8年(1996)9月27日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/06			H 0 4 L 9/02	Z
9/14		7368-5E	G 0 6 F 13/00	3 5 1 Z
G 0 6 F 13/00	3 5 1	7259-5 J	G 0 9 C 1/00	
G 0 9 C 1/00		9466-5K	H 0 4 L 11/20	1 0 1 B
H 0 4 L 12/54				

審査請求 未請求 請求項の数13 O L (全 20 頁) 最終頁に続く

(21) 出願番号 特願平7-52252

(22) 出願日 平成7年(1995)3月13日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 西岡 玄次

神奈川県川崎市麻生区王禅時1099番地株式

会社日立製作所システム開発研究所内

(72) 発明者 宮崎 聡

神奈川県川崎市麻生区王禅時1099番地株式

会社日立製作所システム開発研究所内

(74) 代理人 弁理士 小川 勝男

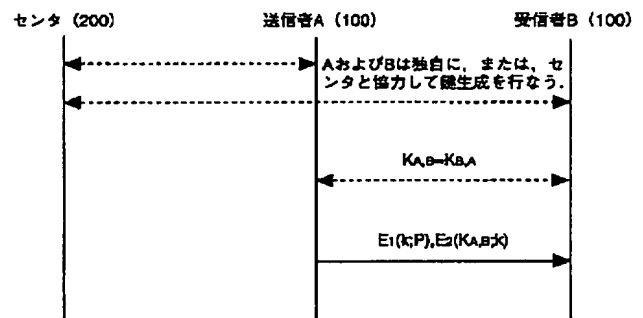
(54) 【発明の名称】 電子メール暗号化方法及び暗号化システム

(57) 【要約】

【目的】 メールシステムや機種に特定しないで通常のメールと併用することができ、電子メールの送信者および受信者双方のセキュリティ機能実現のための計算処理およびメモリの負担が少なく、かつ、利用者の鍵の一致の心配がない盗聴や不正者のなりすましに対して安全性の高い電子メール暗号化方法を提供する。

【構成】 通信ネットワークの各利用者は各々の鍵情報を作成し、公開鍵のみを公開する。次に、電子メールの送信者および受信者はそれぞれ自分の秘密鍵と相手の公開鍵からマスタ鍵 $K_{A,B}$ 、 $K_{B,A}$ の共有を行ない、送信者は秘密鍵暗号を用いて、メール本文 P をデータ暗号化鍵 k で暗号化し、データ暗号化鍵をマスタ鍵で暗号化し、それらを受信者に送り、受信者はマスタ鍵 $K_{B,A}$ を用いてデータ暗号化鍵 k を復号化し、さらにデータ暗号化鍵 k からメール本文 P を復号化する。

図 2



1

【特許請求の範囲】

【請求項1】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、準備処理として、送信者Aは秘密鍵 x_A および秘密鍵 x_A に対応する公開鍵 y_A を作成し、受信者Bは秘密鍵 x_B および秘密鍵 x_B に対応する公開鍵 y_B を作成し、それぞれ公開鍵のみを公開し、マスタ鍵共有処理として、送信者Aは自分の秘密鍵 x_A と受信者Bの公開鍵 y_B からマスタ鍵 $K_{A,B}$ を作成し、受信者Bは自分の秘密鍵 x_B と受信者Bの公開鍵 y_A からマスタ鍵 $K_{B,A}$ を作成し、このとき、 $K_{A,B}=K_{B,A}$ が成立し、特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスタ鍵、または、各マスタ鍵を送信者Aの秘密鍵から作成した鍵を用いて暗号化した情報を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし、メール本文の暗復号化処理として、送信者Aはデータ暗号化鍵 k をランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文 P をデータ暗号化鍵 k にて暗号化した暗号文 $E_1(k; P)$ と、データ暗号化鍵 k をマスタ鍵 $K_{A,B}$ にて暗号化した暗号文 $E_2(K_{A,B}; k)$ を受信者Bに送信し、受信者Bは、マスタ鍵 $K_{B,A}$ を用いて $E_2(K_{A,B}; k)$ からデータ暗号化鍵 k を復号化し、さらにデータ暗号化鍵 k を用いて $E_1(k; P)$ からメール本文 P を復号化することを特徴とする電子メール暗号化方法。

【請求項2】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、準備処理として、センタはセンタの秘密情報として1対1関数 f を作成し、送信者Aは秘密鍵 x_A および秘密鍵 x_A に対応する公開鍵 y_A を作成し、受信者Bは秘密鍵 x_B および秘密鍵 x_B に対応する公開鍵 y_B を作成し、センタへの登録処理として、送信者Aおよび受信者Bは自分のID情報をセンタに登録し、センタはセンタの秘密情報である関数 f を用いて、送信

$$y_{Aj} = \exp(a : x_{Aj}) \pmod{p} \text{ for } j = 1, \dots, n, \dots \text{ (数1)}$$

を計算し、 y_{Aj} ($j = 1, \dots, n$)を送信者Aの公開鍵として登録し、

受信者Bは、 $0 < x_{Bj} < p-1$ なる整数 x_{Bj} ($j = 1,$

$$y_{Bj} = \exp(a : x_{Bj}) \pmod{p} \text{ for } j = 1, \dots, n, \dots \text{ (数2)}$$

を計算し、 y_{Bj} ($j = 1, \dots, n$)を受信者Bの公開鍵として登録し(ただし、 $\exp(a : x)$ は a を x 乗した値を表わす)、マスタ鍵共有処理として、

送信者Aは、自分の秘密鍵である整数 x_{Aj} と受信者Bの

$$K_{A,B} = \Pi \{ \exp(y_{Bj} : x_{Aj}) \pmod{p} \mid j = 1, \dots, n \},$$

2

者AのID情報 I_A から送信者Aに固有の秘密鍵 s_A を、 $s_A = f(I_A)$ 、で作成し、同様に受信者BのID情報 I_B から受信者Bに固有の秘密鍵 s_B を、 $s_B = f(I_B)$ 、で作成し、センタは秘密鍵 s_A と s_A に対応する公開鍵 v_A の組 (s_A, v_A) を送信者Aに安全に配布し、同様に秘密鍵 s_B と s_B に対応する公開鍵 v_B の組 (s_B, v_B) を受信者Bに安全に配布し、このとき、 $I_A \neq I_B$ ならば $s_A \neq s_B$ かつ $v_A \neq v_B$ 、が成立し、送信者Aは (y_A, v_A) を、受信者Bは (y_B, v_B) をそれぞれ自分の公開情報として登録し、マスタ鍵の共有処理として、送信者Aは自分の秘密鍵 (x_A, s_A) と受信者Bの公開鍵 (y_B, v_B) からマスタ鍵 $K_{A,B}$ を作成し、受信者Bは自分の秘密鍵 (x_B, s_B) と受信者Bの公開鍵 (y_A, v_A) からマスタ鍵 $K_{B,A}$ を作成し、このとき、 $K_{A,B} = K_{B,A}$ が成立し、特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスタ鍵、または、各マスタ鍵を送信者Aの秘密鍵から作成した鍵を用いて暗号化した情報、を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし、メール本文の暗復号化処理として、送信者Aはデータ暗号化鍵 k をランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文 P をデータ暗号化鍵 k にて暗号化した暗号文 $E_1(k; P)$ と、データ暗号化鍵 k をマスタ鍵 $K_{A,B}$ にて暗号化した暗号文 $E_2(K_{A,B}; k)$ を受信者Bに送信し、受信者Bは、マスタ鍵 $K_{B,A}$ を用いて $E_2(K_{A,B}; k)$ からデータ暗号化鍵 k を復号化し、さらにデータ暗号化鍵 k を用いて $E_1(k; P)$ からメール本文 P を復号化することを特徴とする電子メール暗号化方法。

【請求項3】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、準備処理として、送信者Aは、 $0 < x_{Aj} < p-1$ なる整数 x_{Aj} ($j = 1, \dots, n$)をランダムに選び、公開情報である整数 a 、素数 p を用いて、

【数1】

\dots, n)をランダムに選び、

【数2】

公開鍵である y_{Bj} ($j = 1, \dots, n$)を用いて、マスタ鍵 $K_{A,B}$ を、

【数3】

にて作成し、

受信者Bは、自分の秘密鍵である整数 x_{Bj} と送信者Aの公開鍵である y_{Aj} ($j=1, \dots, n$)を用いて、マスタ

$$K_{B,A} = \prod \{ \exp(y_{Aj} : x_{Bj}) \pmod{p} \mid j=1, \dots, n \},$$

にて作成し、

このとき、 $K_{A,B} = K_{B,A}$ が成立し、特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスタ鍵からなる集合

S_A 、または、送信者Aの秘密鍵である整数 x_{Aj} ($j=1, \dots, n$)と鍵生成関数 θ から、

$$\text{【数5】 } K(A) = \theta(x_{A1}, \dots, x_{An}),$$

にて作成した鍵 $K(A)$ を用いてマスタ鍵の集合 S_A を暗号化した

$$C(A) = E_A(K(A); S_A),$$

を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし(ただし、 $E_A(k; M)$ はAが所持する秘密鍵暗号アルゴリズムにより明文Mを鍵kにて暗号化した結果を表わす)、

メール本文の暗復号化処理として、送信者Aは、データ暗号化鍵kをランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文Pをデータ暗号化鍵kにて暗号化した暗号文 $E(k; P)$ と、データ暗号化鍵kをマスタ鍵 $K_{A,B}$ にて暗号化した暗号文 $E(K_{A,B}; k)$ をメール受信者Bに送信し、受信者Bは、マスタ鍵 $K_{B,A}$ を用いて $E(K_{A,B}; k)$ からデータ暗号化鍵kを復号化し、さらにデータ暗号化鍵kを用いて $E(k; P)$ からメール本文Pを復号化することを特徴とする電子メール暗号化方法。

【請求項4】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、

準備処理として、センタは、素数 p_1 と、 p_2-1 が二つの大きな素数を因数として持つ素数 p_2 と、整数 a_1 、 a_2 を公開し、 p_2-1 の素因数分解を秘密とし、送信者Aは、 $0 < x_A < p_1-1$ なる整数 x_A をランダムに選び、

$$\text{【数6】 } y_A = \exp(a_1 : x_A) \pmod{p_1},$$

を計算し、

受信者Bは、 $0 < x_B < p_1-1$ なる整数 x_B をランダムに選び、

$$\text{【数7】 } y_B = \exp(a_1 : x_B) \pmod{p_1},$$

を計算し(ただし、 $\exp(a : x)$ はaをx乗した値を表わす。)、

センタへの登録処理として、送信者Aおよび受信者Bは、自分のID情報をセンタに登録し、センタは送信者AのID情報 I_A から、 $I_A + i_A \pmod{p_2-1}$ が平方剰余、かつ、 $I_A \neq I_B$ ならば $I_A + i_A \pmod{p_2-1}$

鍵 $K_{B,A}$ を、

【数4】

$\neq I_B + i_B \pmod{p_2-1}$ となるように正整数 i_A を選び、送信者Aに固有の秘密鍵 s_A を、

$$\text{【数8】 } s_A = \exp(I_A + i_A : 1/2) \pmod{p_2-1},$$

にて計算し、同様に受信者BのID情報 I_B から、送信者Bに固有の秘密鍵 s_B を、

$$10 \text{ 【数9】 } s_B = \exp(I_B + i_B : 1/2) \pmod{p_2-1},$$

にて計算し、各々を送信者Aおよび受信者Bに安全に配布し、このとき、ID情報が異なれば対応する秘密鍵も異なり、送信者Aは y_A と、秘密鍵 s_A に対応する公開鍵

$$\text{【数10】 } v_A = \exp(a_2 : s_A) \pmod{p_2},$$

との組 (y_A, v_A) を送信者Aの公開鍵として登録し、受信者Bは y_B と、秘密鍵 s_B に対応する公開鍵

$$\text{【数11】 } v_B = \exp(a_2 : s_B) \pmod{p_2},$$

との組 (y_B, v_B) を受信者Bの公開鍵として登録し、マスタ鍵共有処理として、送信者Aは、受信者Bとの間で

20 共通に保有する関数gを用いて、自分の秘密鍵である (x_A, s_A) と受信者Bの公開鍵である (y_B, v_B) から、マスタ鍵 $K_{A,B}$ を、

$$\text{【数12】 } K_{A,B} = g(\exp(y_B : x_A) \pmod{p_1}, \exp(v_B : s_A) \pmod{p_2}),$$

にて作成し、受信者Bは、自分の秘密鍵である (x_B, s_B) と送信者Aの公開鍵である (y_A, v_A) を用いて、マスタ鍵 $K_{B,A}$ を、

$$\text{【数13】 } K_{B,A} = g(\exp(y_A : x_B) \pmod{p_1}, \exp(v_A : s_B) \pmod{p_2}),$$

30 にて作成し、

このとき、 $K_{A,B} = K_{B,A}$ が成立し、特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスタ鍵からなる集合 S_A 、または、送信者Aの秘密鍵 (x_A, s_A) と鍵生成関数 θ から、

$$\text{【数14】 } K(A) = \theta(x_A, s_A),$$

にて作成した鍵 $K(A)$ を用いてマスタ鍵の集合 S_A を暗号化した

$$\text{【数15】 } C(A) = E_A(K(A); S_A),$$

40 を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし(ただし、 $E_A(k; M)$ はAが所持する秘密鍵暗号アルゴリズムにより明文Mを鍵kにて暗号化した結果を表わす。)、

メール本文の暗復号化処理として、送信者Aは、データ暗号化鍵kをランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文Pをデータ暗号化鍵kにて暗号化した暗号文 $E(k;$

50

5

P)と、データ暗号化鍵 k をマスク鍵 $K_{A,B}$ にて暗号化した暗号文 $E(K_{A,B}; k)$ をメール受信者Bに送信し、受信者Bは、マスク鍵 $K_{B,A}$ を用いて $E(K_{A,B}; k)$ からデータ暗号化鍵 k を復号化し、さらにデータ暗号化鍵 k を用いて $E(k; P)$ からメール本文 P を復号化することを特徴とする電子メール暗号化方法。

【請求項5】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、

準備処理として、センタは、素数 p_1 と、 p_2-1 が二つの大きな素数を因数として持つ素数 p_2 と、整数 a_1 、 a_2 を公開し、 p_2-1 の素因数分解を秘密とし、送信者Aは、 $0 < x_A < p_1-1$ なる整数 x_A をランダムに選び、

【数16】 $y_A = \exp(a_1 : x_A) \pmod{p_1}$,

を計算し、受信者Bは、 $0 < x_B < p_1-1$ なる整数 x_B をランダムに選び、

【数17】 $y_B = \exp(a_1 : x_B) \pmod{p_1}$,

を計算し、センタへの登録処理として、送信者Aおよび受信者Bは、自分のID情報をセンタに登録し、センタは送信者AのID情報 I_A から、送信者Aに固有の秘密鍵 s_A を正数 e を用いて、

【数18】 $s_A = \exp(I_A : e) \pmod{p_2-1}$,

にて計算し、同様に受信者BのID情報 I_B から、送信者Bに固有の秘密鍵 s_B を正数 e を用いて、

【数19】 $s_B = \exp(I_B : e) \pmod{p_2-1}$,

にて計算し、各々を送信者Aおよび受信者Bに安全に配布し(ただし、 $\exp(a : x)$ は a を x 乗した値を表わす)、

このとき、ID情報が異なれば対応する秘密鍵も異なり、送信者Aは y_A と、秘密鍵 s_A に対応する公開鍵

【数20】 $v_A = \exp(a_2 : s_A) \pmod{p_2}$,

の組 (y_A, v_A) を送信者Aの公開鍵として登録し、受信者Bは y_B と、秘密鍵 s_B に対応する公開鍵

【数21】 $v_B = \exp(a_2 : s_B) \pmod{p_2}$,

の組 (y_B, v_B) を受信者Bの公開鍵として登録し、マスク鍵の共有処理として、送信者Aは、受信者Bとの間で共通に保有する関数 g を用いて、自分の秘密鍵である (x_A, s_A) と受信者Bの公開鍵である (y_B, v_B) から、マスク鍵 $K_{A,B}$ を、

【数22】 $K_{A,B} = g(\exp(y_B : x_A) \pmod{p_1}, \exp(v_B : s_A) \pmod{p_2})$,

にて作成し、受信者Bは、自分の秘密鍵である (x_B, s_B) と送信者Aの公開鍵である (y_A, v_A) を用いて、マスク鍵 $K_{B,A}$ を、

【数23】 $K_{B,A} = g(\exp(y_A : x_B) \pmod{p_1}, \exp(v_A : s_B) \pmod{p_2})$,

にて作成し、このとき、 $K_{A,B} = K_{B,A}$ が成立し、

特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスク

6

鍵からなる集合 S_A 、または、送信者Aの秘密鍵 (x_A, s_A) と鍵生成関数 θ から、

【数24】 $K(A) = \theta(x_A, s_A)$,

にて作成した鍵 $K(A)$ を用いてマスク鍵の集合 S_A を暗号化した

【数25】 $C(A) = E_A(K(A) : S_A)$,

を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスク鍵が必要な場合、マスク鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスク鍵を作成することなく、記憶されているマスク鍵を使うこととし(ただし、 $E_A(k; M)$ はAが所持する秘密鍵暗号アルゴリズムにより明文 M を鍵 k にて暗号化した結果を表わす)、

メール本文の暗復号化処理として、送信者Aは、データ暗号化鍵 k をランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文 P をデータ暗号化鍵 k にて暗号化した暗号文 $E(k; P)$ と、データ暗号化鍵 k をマスク鍵 $K_{A,B}$ にて暗号化した暗号文 $E(K_{A,B}; k)$ をメール受信者Bに送信し、受信者Bは、マスク鍵 $K_{B,A}$ を用いて $E(K_{A,B}; k)$ からデータ暗号化鍵 k を復号化し、さらにデータ暗号化鍵 k を用いて $E(k; P)$ からメール本文 P を復号化することを特徴とする電子メール暗号化方法。

【請求項6】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、準備処理として、センタは、素数 p と合成数 $n = p_1 \cdot p_2$ と整数 a を公開し、 n の素因数分解と正数 α を秘密とし、送信者Aは、 $0 < x_A < p-1$ なる整数 x_A をランダムに選び、

【数26】 $y_A = \exp(a : x_A) \pmod{p}$,

を計算し、受信者Bは、 $0 < x_B < p-1$ なる整数 x_B をランダムに選び、

【数27】 $y_B = \exp(a : x_B) \pmod{p}$,

を計算し、センタへの登録処理として、送信者Aおよび受信者Bは、自分のID情報をセンタに登録し、センタは送信者AのID情報 I_A から、 $I_A + i_A \pmod{1.c.d(p_1-1, p_2-1)}$ が平方剰余、かつ、 $I_A \neq I_B$ ならば $I_A + i_A \pmod{1.c.d(p_1-1, p_2-1)} \neq I_B + i_B \pmod{1.c.d(p_1-1, p_2-1)}$ となるように正整数 i_A を選び、送信者Aに固有の鍵 (s_A, v_A) を、

【数28】 $s_A = \exp(I_A + i_A : 1/2) \pmod{1.c.d(p_1-1, p_2-1)}$,

$v_A = \exp(\alpha : s_A) \pmod{n}$,

にて計算し、同様に受信者BのID情報 I_B から、受信者Bに固有の鍵 (s_B, v_B) を、

【数29】 $s_B = \exp(I_B + i_B : 1/2) \pmod{1.c.d(p_1-1, p_2-1)}$,

$v_B = \exp(\alpha : s_B) \pmod{n}$,

にて計算し、各々を送信者Aおよび受信者Bに安全に配

7

布し(ただし、 $\exp(a : x)$ は a を x 乗した値を表わす)、

このとき、ID情報が異なれば対応する鍵も異なり、送信者Aは(y_A, v_A)を送信者Aの公開鍵として登録し、受信者Bは(y_B, v_B)を受信者Bの公開鍵として登録し、マスタ鍵共有処理として、

送信者Aは、受信者Bとの間で共通に保有する関数 g を用いて、自分の秘密鍵である(x_A, s_A)と受信者Bの公開鍵である(y_B, v_B)から、マスタ鍵 $K_{A,B}$ を、

【数30】 $K_{A,B} = g(\exp(y_B : x_A)(\bmod p), \exp(v_B : s_A)(\bmod n))$, 10

にて作成し、受信者Bは、自分の秘密鍵である(x_B, s_B)と送信者Aの公開鍵である(y_A, v_A)を用いてマスタ鍵 $K_{B,A}$ を、

【数31】 $K_{B,A} = g(\exp(y_A : x_B)(\bmod p), \exp(v_A : s_B)(\bmod n))$,

にて作成し、このとき、 $K_{A,B} = K_{B,A}$ が成立し、特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスタ鍵からなる集合 S_A 、または、送信者Aの秘密鍵(x_A, s_A)と鍵生成関数 θ から、

【数32】 $K(A) = \theta(x_A, s_A)$,

にて作成した鍵 $K(A)$ を用いてマスタ鍵の集合 S_A を暗号化した

【数33】 $C(A) = E_A(K(A) ; S_A)$,

を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし(ただし、 $E_A(k ; M)$ はAが所持する秘密鍵暗号アルゴリズムにより平文 M を鍵 k にて暗号化した結果を表わす)、

メール本文の暗復号化処理として、送信者Aは、データ暗号化鍵 k をランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文 P をデータ暗号化鍵 k にて暗号化した暗号文 $E(k ; P)$ と、データ暗号化鍵 k をマスタ鍵 $K_{A,B}$ にて暗号化した暗号文 $E(K_{A,B} ; k)$ をメール受信者Bに送信し、受信者Bは、マスタ鍵 $K_{B,A}$ を用いて $E(K_{A,B} ; k)$ からデータ暗号化鍵 k を復号化し、さらにデータ暗号化鍵 k を用いて $E(k ; P)$ からメール本文 P を復号化することを特徴とする電子メール暗号化方法。

【請求項7】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、

準備処理として、センタは、素数 p と合成数 $n = p_1 \cdot p_2$ と整数 a を公開し、 n の素因数分解と正数 α を秘密とし、送信者Aは、 $0 < x_A < p - 1$ なる整数 x_A をランダムに選び、

8

【数34】 $y_A = \exp(a : x_A)(\bmod p)$,

を計算し、受信者Bは、 $0 < x_B < p - 1$ なる整数 x_B をランダムに選び、

【数35】 $y_B = \exp(a : x_B)(\bmod p)$,

を計算し、センタへの登録処理として、送信者Aおよび受信者Bは、自分のID情報をセンタに登録し、センタは送信者AのID情報 I_A から、送信者Aに固有の鍵(s_A, v_A)を正数 e を用いて、

【数36】 $s_A = \exp(I_A : e)(\bmod \text{l.c.d}(p_1 - 1, p_2 - 1))$,

$v_A = \exp(\alpha : s_A)(\bmod n)$,

にて計算し、同様に受信者BのID情報 I_B から、受信者Bに固有の鍵(s_B, v_B)を、

【数37】 $s_B = \exp(I_B : e)(\bmod \text{l.c.d}(p_1 - 1, p_2 - 1))$,

$v_B = \exp(\alpha : s_B)(\bmod n)$,

にて計算し、各々を送信者Aおよび受信者Bに安全に配布し(ただし、 $\exp(a : x)$ は a を x 乗した値を表わす)、このとき、ID情報が異なれば対応する秘密鍵も

異なり、送信者Aは(y_A, v_A)を送信者Aの公開鍵として登録し、受信者Bは(y_B, v_B)を受信者Bの公開鍵として登録し、マスタ鍵共有処理として、送信者Aは、受信者Bとの間で共通に保有する関数 g を用いて、

自分の秘密鍵である(x_A, s_A)と受信者Bの公開鍵である(y_B, v_B)から、マスタ鍵 $K_{A,B}$ を、

【数38】 $K_{A,B} = g(\exp(y_B : x_A)(\bmod p), \exp(v_B : s_A)(\bmod n))$,

にて作成し、受信者Bは、自分の秘密鍵である(x_B, s_B)と送信者Aの公開鍵である(y_A, v_A)を用いてマスタ鍵 $K_{B,A}$ を、

【数39】 $K_{B,A} = g(\exp(y_A : x_B)(\bmod p), \exp(v_A : s_B)(\bmod n))$,

にて作成し、このとき、 $K_{A,B} = K_{B,A}$ が成立し、特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスタ鍵からなる集合 S_A 、または、送信者Aの秘密鍵(x_A, s_A)と鍵生成関数 θ から、

【数40】 $K(A) = \theta(x_A, s_A)$,

にて作成した鍵 $K(A)$ を用いてマスタ鍵の集合 S_A を暗号化した

【数41】 $C(A) = E_A(K(A) ; S_A)$,

を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし(ただし、 $E_A(k ; M)$ はAが所持する秘密鍵暗号アルゴリズムにより平文 M を鍵 k にて暗号化した結果を表わす)、

メール本文の暗復号化処理として、送信者Aは、データ暗号化鍵 k をランダムに選び、受信者Bとの間で共通に

保有する秘密鍵暗号系アルゴリズムを用いて、メール本文 P をデータ暗号化鍵 k にて暗号化した暗号文 $E(k; P)$ と、データ暗号化鍵 k をマスタ鍵 $K_{A,B}$ にて暗号化した暗号文 $E(K_{A,B}; k)$ をメール受信者 B に送信し、受信者 B は、マスタ鍵 $K_{B,A}$ を用いて $E(K_{A,B}; k)$ からデータ暗号化鍵 k を復号化し、さらにデータ暗号化鍵 k を用いて $E(k; P)$ からメール本文 P を復号化することを特徴とする電子メール暗号化方法。

【請求項8】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者 A が受信者 B に対して送信するメール文を暗号化する電子メール暗号化方法であって、

準備処理として、センタは、素数 p_1, p_2 と整数 a_1, a_2 を公開し、剰余環 $Z/(p_2-1)$ の元を出力する秘密鍵暗号アルゴリズムおよび鍵 r を秘密情報とし（センタの秘密情報である秘密鍵暗号アルゴリズムにより、平文 M を鍵 k で暗号化した結果を $E_0(k; M)$ で表わす）、送信者 A は、 $0 < x_A < p_1-1$ なる整数 x_A をランダムに選び、

【数42】 $y_A = \exp(a_1; x_A) \pmod{p_1}$,
を計算し、受信者 B は、 $0 < x_B < p_1-1$ なる整数 x_B をランダムに選び、

【数43】 $y_B = \exp(a_1; x_B) \pmod{p_1}$,
を計算し（ただし、 $\exp(a; x)$ は a を x 乗した値を表わす）、センタへの登録処理として、送信者 A および受信者 B は、自分のID情報をセンタに登録し、センタは送信者 A のID情報 I_A から送信者 A に固有の秘密鍵 s_A を、

【数44】 $s_A = E_0(r; I_A)$,
にて計算し、同様に受信者 B のID情報 I_B から、送信者 B に固有の秘密鍵 s_B を、

【数45】 $s_B = E_0(r; I_B)$,
にて計算し、各々を送信者 A および受信者 B に安全に配布し、このとき、ID情報が異なれば対応する秘密鍵も異なり、送信者 A は、 y_A と、秘密鍵 s_A に対応する公開鍵

【数46】 $v_A = \exp(a_2; s_A) \pmod{p_2}$,
の組 (y_A, v_A) を送信者 A の公開鍵として登録し、受信者 B は、 y_B と、秘密鍵 s_B に対応する公開鍵

【数47】 $v_B = \exp(a_2; s_B) \pmod{p_2}$,
の組 (y_B, v_B) を受信者 B の公開鍵として登録し、マスタ鍵の共有処理として、送信者 A は、受信者 B との間で共通に保有する関数 g を用いて、自分の秘密鍵である (x_A, s_A) と受信者 B の公開鍵である (y_B, v_B) から、マスタ鍵 $K_{A,B}$ を、

【数48】 $K_{A,B} = g(\exp(y_B; x_A) \pmod{p_1}, \exp(v_B; s_A) \pmod{p_2})$,
にて作成し、受信者 B は、自分の秘密鍵である (x_B, s_B) と送信者 A の公開鍵である (y_A, v_A) を用いて、マスタ鍵 $K_{B,A}$ を、

【数49】 $K_{B,A} = g(\exp(y_A; x_B) \pmod{p_1}, \exp(v_A; s_B) \pmod{p_2})$,
にて作成し、このとき、 $K_{A,B} = K_{B,A}$ が成立し、特に、送信者 A は電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者 A 間の各マスタ鍵からなる集合 S_A 、または、送信者 A の秘密鍵 (x_A, s_A) と鍵生成関数 θ から、

【数50】 $K(A) = \theta(x_A, s_A)$,
にて作成した鍵 $K(A)$ を用いてマスタ鍵の集合 S_A を暗号化した

【数51】 $C(A) = E_A(K(A); S_A)$,
を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし（ただし、 $E_A(k; M)$ は A が所持する秘密鍵暗号アルゴリズムにより平文 M を鍵 k にて暗号化した結果を表わす）、

メール本文の暗復号化処理として、送信者 A は、データ暗号化鍵 k をランダムに選び、受信者 B との間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文 P をデータ暗号化鍵 k にて暗号化した暗号文 $E(k; P)$ と、データ暗号化鍵 k をマスタ鍵 $K_{A,B}$ にて暗号化した暗号文 $E(K_{A,B}; k)$ をメール受信者 B に送信し、受信者 B は、マスタ鍵 $K_{B,A}$ を用いて $E(K_{A,B}; k)$ からデータ暗号化鍵 k を復号化し、さらにデータ暗号化鍵 k を用いて $E(k; P)$ からメール本文 P を復号化することを特徴とする電子メール暗号化方法。

【請求項9】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者 A が受信者 B に対して送信するメール文を暗号化する電子メール暗号化方法であって、準備処理として、センタは、素数 p と合成数 $n = p_1 \cdot p_2$ と整数 a を公開し、整数 α および剰余環 $Z/(N)$ の元を出力する秘密鍵暗号アルゴリズムおよび鍵 r を秘密情報とし（ただし、 $N = \text{l.c.d}(p_1-1, p_2-1)$ であり、センタの秘密情報である秘密鍵暗号アルゴリズムにより平文 M を鍵 k で暗号化した結果を $E_0(k; M)$ で表わす）、送信者 A は、 $0 < x_A < p-1$ なる整数 x_A をランダムに選び、

【数52】 $y_A = \exp(a; x_A) \pmod{p}$,
を計算し、受信者 B は、 $0 < x_B < p-1$ なる整数 x_B をランダムに選び、

【数53】 $y_B = \exp(a; x_B) \pmod{p}$,
を計算し、センタへの登録処理として、送信者 A および受信者 B は、自分のID情報をセンタに登録し、センタは送信者 A のID情報 I_A から送信者 A に固有の鍵 (s_A, v_A) を、

【数54】 $s_A = E_0(r; I_A)$,
 $v_A = \exp(\alpha; s_A) \pmod{n}$,
50

にて計算し、同様に受信者BのID情報 I_B から受信者Bに固有の鍵(s_B, v_B)を、

【数55】 $s_B = E_0(r; I_B)$,

$v_B = \exp(\alpha; s_B) \pmod{n}$,

にて計算し、各々を送信者Aおよび受信者Bに安全に配布し、このとき、ID情報が異なれば対応する鍵も異なり、送信者Aは(y_A, v_A)を送信者Aの公開鍵として登録し、受信者Bは(y_B, v_B)を受信者Bの公開鍵として登録し、マスタ鍵共有処理として、

送信者Aは、受信者Bとの間で共通に保有する関数 g を用いて、自分の秘密鍵である(x_A, s_A)と受信者Bの公開鍵である(y_B, v_B)から、マスタ鍵 $K_{A,B}$ を、

【数56】 $K_{A,B} = g(\exp(y_B; x_A) \pmod{p}, \exp(v_B; s_A) \pmod{n})$,

にて作成し、受信者Bは、自分の秘密鍵である(x_B, s_B)と送信者Aの公開鍵である(y_A, v_A)を用いてマスタ鍵 $K_{B,A}$ を、

【数57】 $K_{B,A} = g(\exp(y_A; x_B) \pmod{p}, \exp(v_A; s_B) \pmod{n})$,

にて作成し、このとき、 $K_{A,B} = K_{B,A}$ が成立し、特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスタ鍵からなる集合 S_A 、または、送信者Aの秘密鍵(x_A, s_A)と鍵生成関数 θ から、

【数58】 $K(A) = \theta(x_A, s_A)$,

にて作成した鍵 $K(A)$ を用いてマスタ鍵の集合 S_A を暗号化した

【数59】 $C(A) = E_A(K(A); S_A)$,

を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし(ただし、 $E_A(k; M)$ はAが所持する秘密鍵暗号アルゴリズムにより平文 M を鍵 k にて暗号化した結果を表わす)、

メール本文の暗復号化処理として、送信者Aは、データ暗号化鍵 k をランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文 P をデータ暗号化鍵 k にて暗号化した暗号文 $E(k; P)$ と、データ暗号化鍵 k をマスタ鍵 $K_{A,B}$ にて暗号化した暗号文 $E(K_{A,B}; k)$ をメール受信者Bに送信し、受信者Bは、マスタ鍵 $K_{B,A}$ を用いて $E(K_{A,B}; k)$ からデータ暗号化鍵 k を復号化し、さらにデータ暗号化鍵 k を用いて $E(k; P)$ からメール本文 P を復号化することを特徴とする電子メール暗号化方法。

【請求項10】請求項4、5、6、7、8または9において、

マスタ鍵共有処理の中で、送信者Aと受信者Bとの間で共通に保有する関数 g として、

【数60】 $g(x_1, x_2) = h(\phi(x_1, x_2))$,

なる関数を用いて(ただし、 h はハッシュ関数、 ϕ は、
【数61】 $\phi: Z/(p) \times Z/(n) \rightarrow Z/(pn)$
 $((x, x) \rightarrow x)$,

なる同型写像を表わし、 $Z/(m)$ は整数 m を法とする剰余環を表わし、 x はそれぞれの剰余環において x を代表元とする剰余類を表わす。)、マスタ鍵を作成する電子メール暗号化方法。

【請求項11】請求項4、5、6、7、8または9において、マスタ鍵共有処理の中で、送信者Aと受信者Bとの間で共通に保有する関数 g として、

【数62】 $g(x_1, x_2) = h(x_1 * x_2)$,

なる関数を用いて(ただし、 h はハッシュ関数、 $x_1 * x_2$ は x_1 と x_2 の排他的論理和を表わす)、マスタ鍵を作成する電子メール暗号化方法。

【請求項12】請求項3、4、5、6、7、8、9または11において、

メール本文の暗復号化処理として、送信者Aは、データ暗号化鍵 k をランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文 P をデータ暗号化鍵 k にて暗号化した暗号文 $E(k; P)$ と、データ暗号化鍵 k とマスタ鍵 $K_{A,B}$ の排他的論理和 $k * K_{A,B}$ を受信者Bに送信し、受信者Bは、マスタ鍵 $K_{B,A}$ と $k * K_{A,B}$ の排他的論理和を取ることにより、データ暗号化鍵 k を復号化し、さらにデータ暗号化鍵 k を用いて $E(k; P)$ からメール本文 P を復号化する電子メール暗号化システム。

【請求項13】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、送信者および受信者はそれぞれの秘密鍵を内蔵した演算機能付き記憶媒体を所持し、送信者は通信ネットワークに接続された計算機1と送信者の記憶媒体Aを用いて、請求項1から請求項12の電子メール暗号化方法に従い、暗号化処理を記憶媒体A内で行ない、送信文を計算機1に出力し、計算機1から通信回線を介して受信者の使用する計算機2に送信し、受信者は、送信者から送られてきた送信文を計算機2から受信者の演算機能付き記憶媒体Bに出力し、記憶媒体B内でデータ暗号化鍵およびメール本文を復号化することを特徴とする電子メール暗号化方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、通信ネットワークを介して文書を送受信する電子メール通信システムにおいて、ネットワーク上での盗聴や不正者によるなりすましに対して安全性を向上させた電子メール暗号化方法に関する。

【0002】

【従来の技術】Internetにおける電子メールのセキュリティを強化することを目的として、文献「Linn, J., et

al., "Privacy Enhancement for Internet Electronic Mail: Part I, II, III, IV", RFC-1421-1424, 1993」に記載の P E M (Privacy Enhanced Mail) が提案されている。以下、P E M の電子メール暗号化技法について簡単に説明する。

【0003】P E M では、鍵管理に公開鍵暗号 R S A (参考文献「R. L. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Communications of the ACM, Vol. 21, 1978」) を利用し、データの暗号化に米国暗号標準である秘密鍵暗号 D E S (参考文献「Data Encryption Standard, FIPS-PUB-46, 1977」) を用いている。

【0004】送信者 A は受信者 B にネットワークを介して電子メールを送る。

【0005】Step 1. A はデータ暗号化鍵 K をランダムに作り、鍵 K を用いてメール本文 P を D E S により暗号化する。すなわち、メール本文 P の暗号文 C_1 を、

【0006】

【数63】 $C_1 = E(K; P)$,

とする。

【0007】Step 2. A は B の公開鍵 (e_B, n_B) を用いて鍵 K を R S A により暗号化する。すなわち、鍵 K の暗号文 C_2 を、

【0008】

【数64】 $C_2 = \exp(K; e_B) \pmod{n_B}$,

とする。ただし、 $\exp(a; x)$ は a を x 乗した値を表す。

【0009】Step 3. A はメール本文 P を公開情報であるハッシュ関数 f を用いて圧縮し、A の秘密鍵 d_A と公開鍵 n_A を用いて $f(P)$ に R S A 署名を行なう。すなわち、 $f(P)$ に対する署名文 $\text{sgn}_A(P)$ を、

【0010】

【数65】 $\text{sgn}_A(P) = \exp(f(P); d_A) \pmod{n_A}$,
とする。

【0011】Step 4. A は $C_1, C_2, \text{sgn}_A(P)$ を B に送る。

【0012】Step 5. B は自分の秘密鍵 d_B を用いて、 C_2 から、

【0013】

【数66】 $K = \exp(C_2; d_B) \pmod{n_B}$,
により、データ暗号化鍵 K を復号化する。

【0014】Step 6. B は鍵 K を用いて、

【0015】

【数67】 $P = D(K; C_1)$,

により、メール本文 P を復号化する。

【0016】Step 7. B はメール本文 P が A から送られてきたことを確かめるため、ハッシュ関数 f と A の公開鍵 (e_A, n_A) を用いて、

【0017】

【数68】 $f(P) = \exp(\text{sgn}_A(P); e_A) \pmod{n_A}$,

を確認する。

【0018】P E M には次の問題点が考えられる。

【0019】(1) 安全性の立場から、データ暗号化鍵は頻繁に変更することが望ましい。P E M の場合、電子メール通信をする機会が多い相手であっても、データ暗号化鍵を変更する度に相手の公開鍵を用いて R S A 暗号により新しいデータ暗号化鍵を暗号化して送らなければならない。特に、一度に多数の相手にメールを送信した場合、R S A 暗号は暗号化のための計算量が比較的大きいため、データ暗号化鍵の暗号化のための計算処理負担が大きい。

【0020】(2) R S A 暗号を用いた鍵配送では、鍵の復号化は受信者の秘密鍵のみで行なわれるため認証機能はない。そのため、P E M では、R S A を用いたデジタル署名を付加することで認証機能を実現している。しかし、デジタル署名は作成と検証のための計算処理負担が大きく、さらに、メール暗号文に付加するヘッダ情報が大きくなる欠点を持つ。

【0021】(3) P E M においては、ネットワークの各利用者の鍵は利用者自身が作成するため、偶然にも異なる利用者の鍵が一致してしまう可能性がある。たとえば、利用者 A と利用者 B の鍵が一致していることに、A が B の公開鍵から気が付くと、A は B になりすましたり、B と他の利用者の電子メール通信を盗聴することができる。

【0022】

【発明が解決しようとする課題】本発明の目的は、通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、メールシステムや機種に特定しないで通常のメールと併用できる特徴を有し、かつ、電子メールの送信者および受信者双方におけるセキュリティ機能実現のための計算処理およびメモリ負担が少なく、かつ、利用者の鍵の一致の心配がない盗聴や不正者のなりすましに対して安全性の高い電子メール暗号化方法を提案することにある。

【0023】

【課題を解決するための手段】本発明は、通信ネットワーク上でデータの送受信を行なう電子メール通信システムにおいて、高効率・高安全な電子メール暗号化方法を提案するものである。

【0024】具体的実現方法の 1 つとしては、送信者 A が受信者 B に対して送信するメール文を暗号化する電子メール暗号化方法であって、

準備処理

センタは、素数 p と合成数 $n = p_1 \cdot p_2$ と整数 a を公開し、 n の素因数分解と正数 α を秘密とする。

【0025】送信者 A は、 $0 < x_A < p-1$ なる整数 x_A をランダムに選び、

【0026】

【数69】 $y_A = \exp(a; x_A) \pmod{p}$,

を計算し、受信者Bは、 $0 < x_B < p-1$ なる整数 x_B をランダムに選び、

【0027】

【数70】 $y_B = \exp(a : x_B) \pmod{p}$,

を計算する。ただし、 $\exp(a : x)$ は a を x 乗した値を表わす。

【0028】 センタへの登録処理

送信者Aおよび受信者Bは、自分のID情報をセンタに登録し、センタは送信者AのID情報 I_A から、送信者Aに固有の鍵 (s_A, v_A) を正数 e を用いて、

【0029】

【数71】 $s_A = \exp(I_A : e) \pmod{1.c.d(p_1-1, p_2-1)}$,

$v_A = \exp(\alpha : s_A) \pmod{n}$,

にて計算し、同様に受信者BのID情報 I_B から、受信者Bに固有の鍵 (s_B, v_B) を、

【0030】

【数72】 $s_B = \exp(I_B : e) \pmod{1.c.d(p_1-1, p_2-1)}$,

$v_B = \exp(\alpha : s_B) \pmod{n}$,

にて計算し、各々を送信者Aおよび受信者Bに安全に配布する。ただし、 $1.c.d(x, y)$ は整数 x, y の最小公倍数を表わす。

【0031】このとき、ID情報が異なれば対応する秘密鍵も異なる。

【0032】送信者Aは (y_A, v_A) を送信者Aの公開鍵として登録し、受信者Bは (y_B, v_B) を受信者Bの公開鍵として登録する。

【0033】 マスタ鍵共有処理

送信者Aは、受信者Bとの間で共通に保有する関数 g を用いて、自分の秘密鍵である (x_A, s_A) と受信者Bの公開鍵である (y_B, v_B) から、マスタ鍵 $K_{A,B}$ を、

【0034】

【数73】 $K_{A,B} = g(\exp(y_B : x_A) \pmod{p}, \exp(v_B : s_A) \pmod{n})$,

にて作成し、受信者Bは、自分の秘密鍵である (x_B, s_B) と送信者Aの公開鍵である (y_A, v_A) を用いてマスタ鍵 $K_{B,A}$ を、

【0035】

【数74】 $K_{B,A} = g(\exp(y_A : x_B) \pmod{p}, \exp(v_A : s_B) \pmod{n})$,

にて作成する。

【0036】このとき、 $K_{A,B} = K_{B,A}$ が成立する。

【0037】特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスタ鍵からなる集合 S_A 、または、送信者Aの秘密鍵 (x_A, s_A) と鍵生成関数 θ から、

【0038】

【数75】 $K(A) = \theta(x_A, s_A)$,

にて作成した鍵 $K(A)$ を用いてマスタ鍵の集合 S_A を暗

号化した

【0039】

【数76】 $C(A) = E_A(K(A) : S_A)$,

を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使う。ただし、 $E_A(k : M)$ はAが所持する秘密鍵暗号アルゴリズムにより平文 M を鍵 k にて暗号化した結果を表わす。

【0040】 メール本文の暗復号化处理

送信者Aは、データ暗号化鍵 k をランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文 P をデータ暗号化鍵 k にて暗号化した暗号文 $E(k : P)$ と、データ暗号化鍵 k をマスタ鍵 $K_{A,B}$ にて暗号化した暗号文 $E(K_{A,B} : k)$ をメール受信者Bに送信する。

【0041】受信者Bは、マスタ鍵 $K_{B,A}$ を用いて $E(K_{A,B} : k)$ からデータ暗号化鍵 k を復号化し、さらにデータ暗号化鍵 k を用いて $E(k : P)$ からメール本文 P を復号化する。

【0042】

【作用】本発明における電子メール暗号化方法では、電子メールの送信者および受信者はそれぞれ自分の秘密鍵と相手の公開鍵からマスタ鍵の共有を行ない、秘密鍵暗号を用いてメール本文の暗号化およびデータ暗号化鍵の配送を行なうことにより、セキュリティ機能実現のための送受信者双方の計算処理負担を削減し、かつ、デジタル署名などの付加情報を付けることなく送信者の認証を実現した。特に、頻繁にメール通信を行なう相手については鍵情報としてマスタ鍵のみを記憶しておけば、受信者の公開鍵の必要もなく、かつ、データ暗号化鍵の更新の度にマスタ鍵の生成を行なう必要もなく、高速な暗号化处理が可能となった。

【0043】また、ID情報は利用者（電子メールの送信者および受信者）毎に異なることを利用して、センタと利用者が協力して利用者の鍵生成を行なうことで、利用者の鍵が一致することがなく、盗聴や不正者のなりすましに対して高い安全性を実現した。

【0044】

【実施例】以下、図面を用いて、本発明の実施例について詳しく説明する。

【0045】図1は、本発明の実施例のシステム構成を示す図である。同図のシステムは、複数の利用者側装置100とセンタ側装置200とから構成されている。利用者側装置100は互いに通信回線300を介して接続されている。

【0046】図2は、本発明における電子メール暗号化方法の概念図を示す。

【0047】図3は、実施例1から9における利用者側装置100の内部構成を示す。利用者側装置100は、乱数発

10

20

30

40

50

生器101、べき乗算器102、鍵生成器103、演算器104、暗復号化装置105、ハッシュ計算器106、メモリ107、通信装置108を備えている。

【0048】図4は、センタ側装置200の内部構成を示す。センタ側装置200は、素数発生器201、原始根生成器202、秘密鍵作成装置203、演算器204を備えている。

【0049】図5は、カード400の内部構成を示す。カード400は、乱数発生器401、べき乗算器402、鍵生成器403、演算器404、暗復号化装置405、ハッシュ計算器406、メモリ407、出力装置408を備えている。

【0050】図6は、実施例10における利用者側装置500の内部構成を示す。利用者側装置500は、カード読取装置501、通信装置502を備えている。

【0051】ネットワークの利用者は通信回線に接続された自分の利用者側装置100（カード400と利用者側装置500）を用いて他の利用者側装置100（カード400と利用者側装置500）を使用する別の利用者に対して電子メール通信を行なうケースを考える。

【0052】このとき、電子メールの暗号化方法について

$$\cdot x_{\lambda j} \in \mathbb{Z} \text{ s.t. } 0 < x_{\lambda j} < p-1 \text{ for } j = 1, \dots, n.$$

公開鍵：

【0058】

$$\cdot y_{\lambda j} = \exp(a : x_{\lambda j}) \pmod{p} \text{ for } j = 1, \dots, n.$$

ただし、 p は素数、 a は $0 < a < p$ で $\mathbb{Z}/(p)$ の原始根となる整数、 n はセキュリティパラメータを表わし、予め与えられているものとする。

【0059】さらに、ネットワークに接続された利用者側装置100内には同一の秘密鍵暗号系アルゴリズムを内蔵した暗復号化装置104があり、この秘密鍵暗号系アルゴリズムを用いて平文 M を鍵 K で暗号化した結果および復号化した結果をそれぞれ $E(K; M)$ 、 $D(K; M)$ で表わす。

【0060】 マスタ鍵の共有

ネットワークの利用者である A 、 B について、 A は B に対して電子メールを送りたい。この目的の下で、 A 、 B は次の手順を実行する。

【0061】 A は A の利用者側装置100A内のべき乗算器102Aおよび演算器104Aを用いて自分の秘密鍵 x_{Aj} と B の公開鍵 y_{Bj} ($j = 1, \dots, n$) からマスタ鍵 $K_{A,B}$ を、

【0062】

$$\text{【数79】 } K_{A,B} = \prod \{ \exp(y_{Bj} : x_{Aj}) \pmod{p} \mid j = 1, \dots, n \},$$

にて計算する。ただし、記号100A等については、数字の後のアルファベットにより利用者の識別を行なう。

【0063】同様にして、 B は B の利用者側装置100B内のべき乗算器102Bおよび演算器104Bを用いて自分の秘密鍵 x_{Bj} と A の公開鍵 y_{Aj} ($j = 1, \dots, n$) からマスタ鍵 $K_{B,A}$ を、

【0064】

$$\text{【数80】 } K_{B,A} = \prod \{ \exp(y_{Aj} : x_{Bj}) \pmod{p} \mid j =$$

て以下の実施例において詳しく説明する。

【0053】 \mathbb{Z} は整数環を表わし、 $\mathbb{Z}/(n)$ は整数 n を法とする剰余環を表わす。特に、 n が素数のとき、 $\mathbb{Z}/(n)$ は剰余体になる。 $x \in \mathbb{Z}$ に対して、 x は対応する剰余環における x を代表元とする剰余類を表わす。また、 $\exp(a : x)$ は a を x 乗した値を表わす。

【0054】ネットワークの利用者のID情報はすべて t ビット以下で表わされる場合、利用者のID情報は $\mathbb{Z}/(\exp(2 : t) - 1)$ の元と考えることができる。このとき、利用者のID情報の集合 Λ を、 $\Lambda = \mathbb{Z}/(\exp(2 : t) - 1)$ と定義する。

【0055】（実施例1）

準備

ネットワークの各利用者 λ はそれぞれ自身の利用者側装置100内の乱数発生器101およびべき乗算器102を用いて次の情報を作成し、公開鍵のみを公開・登録する。

【0056】秘密鍵：

【0057】

【数77】

【数78】

$1, \dots, n\}$ 、

にて作成する。このとき、明らかに、

【0065】

【数81】 $K_{A,B} = K_{B,A}$ 、

が成立する。

【0066】さらに、 A は電子メールを送信する機会が多い利用者に対しては、それらの利用者と A 間の各マスタ鍵の集合 S_A 、または、 A の秘密情報 x_{Aj} ($j = 1, \dots, n$) から利用者側装置100A内の鍵生成器103Aにより鍵 $K(A)$ を作成し、暗復号化装置105Aを用いて鍵 $K(A)$ により S_A を暗号化した

【0067】

【数82】 $C(A) = E(K(A) : S_A)$ 、

を、メモリ107Aに記憶する。以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに自分の秘密鍵と相手の公開鍵からマスタ鍵を作成することなく、メモリ107Aに記憶されているマスタ鍵を使う。

【0068】 メール本文の暗号化

A は、利用者側装置100A内の乱数発生器101Aを用いて乱数 r を選び、 r を入力として鍵生成器103Aからデータ暗号化鍵 k を作成する。メール本文 P を暗復号化装置105Aを用いてデータ暗号化鍵 k により暗号化した暗号文 C_1 を、

【0069】

【数83】 $C_1 = E(k : P)$ 、

にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵 k をマスタ鍵 $K_{A,B}$ で暗号化した暗号文 C_2 を、

【0070】

【数84】 $C_2 = E(K_{A,B}; k)$,

にて作成する。

【0071】 Aは、通信装置108Aを用いて C_1 と C_2 を B に送る。

【0072】 メール本文の復号化

Bは送られてきた C_1 と C_2 に対して、Bの利用者側装置100B内の暗復号化装置105Bを用いて、まず、マスタ鍵 $K_{B,A}$ より、

【0073】

【数85】 $k = D(K_{B,A}; C_2)$,

にてデータ暗号化鍵 k を復号化し、次にデータ暗号化鍵 k を用いて、

【0074】

【数86】 $P = D(k; C_1)$,

にて、メール本文 P を復号化する。

【0075】 (実施例2) 実施例2では、センタの存在を仮定して利用者の鍵情報が偶然にも一致することのない高い安全性をもつ電子メール暗号化方法について述べる。

【0076】 準備

センタはセンタ側装置200内の素数発生器201、原始根生成器202および演算器204を用いて次の情報を作成する。

【0077】 公開情報:

- ・ p_1 ; 素数,
- ・ $p_2 = 2q_1q_2 + 1$; 素数,
- ・ $a_1 \in Z$ s.t. $0 < a_1 < p_1$ 、かつ、 a_1 は $Z/(p_1)$ で原始根,
- ・ $a_2 \in Z$ s.t. $0 < a_2 < p_2$ 、かつ、 a_2 は $Z/(p_2)$ で原始根,
- 秘密情報:
- ・ $q_1, q_2 \in Z$; 素数.

ネットワークの各利用者 λ は利用者側装置100内の乱数発生器101およびべき乗算器102を用いて次の鍵を作成する。

【0078】 秘密鍵:

【0079】

【数87】 $x_\lambda \in Z$ s.t. $0 < x_\lambda < p_1 - 1$.

公開鍵:

【0080】

【数88】 $y_\lambda = \exp(a_1; x_\lambda) \pmod{p_1}$.

センタへの登録

ネットワークの利用者 λ はセンタに自分のID情報 I_λ

$$\phi: Z/(p_1) \times Z/(p_2) \rightarrow Z/(n) \quad ((x, x) \rightarrow x),$$

なる同型写像を表わす ($n = p_1 p_2$)。ここで、 x はそれぞれの剰余環における x を代表元とする剰余類を表わす。

を登録する。

【0081】 センタは、センタ側装置200内の秘密鍵作成装置203を用いて、

【0082】

【数89】 $e, d \equiv 1 \pmod{\text{l.c.d}(q_1-1, q_2-1)}$,
なる $e, d \in Z$ を作成し、利用者 λ のID情報 I_λ に対して、

【0083】

【数90】 $s_\lambda = \exp(I_\lambda; e) \pmod{p_2-1}$,
を計算して、 s_λ を利用者 λ に安全に配布する。

【0084】 このとき、

【0085】

【数91】

$s_\lambda \neq s_\mu$ if $I_\lambda \neq I_\mu \in \Lambda = Z/(p_2-1)$,
が成立することに注意する。

【0086】 マスタ鍵の共有

ネットワークの利用者 λ は、ベクトル (y_λ, v_λ) を λ の公開鍵として登録を行なう。ただし、

【0087】

【数92】 $v_\lambda = \exp(a_2; s_\lambda) \pmod{p_2}$.

さらに、ネットワークに接続された利用者側装置100内には同一の秘密鍵暗号系アルゴリズムを内蔵した暗復号化装置105があり、この秘密鍵暗号系アルゴリズムを用いて平文 M を鍵 K で暗号化した結果および復号化した結果をそれぞれ $E(K; M)$, $D(K; M)$ で表わす。

【0088】 ネットワークの利用者 A, B について、A は B に対して電子メールを送りたい。この目的の下で、A, B は次の手順を実行する

A は A の利用者側装置100A内のべき乗算器102Aと演算器104Aとハッシュ計算器106Aを用いて、A の秘密鍵 (x_A, s_A) と B の公開鍵 (y_B, v_B) からマスタ鍵 $K_{A,B}$ を、

【0089】

【数93】 $K_{A,B} = g(\phi(\exp(y_B; x_A) \pmod{p_1}), \exp(v_B; s_A) \pmod{p_2}))$,

にて作成する。同様に、B は B の利用者側装置100B内のべき乗算器102Bと演算器104Bとハッシュ計算器106Bを用いて、B の秘密鍵 (x_B, s_B) と A の公開鍵 (y_A, v_A) からマスタ鍵 $K_{B,A}$ を、

40 【0090】

【数94】 $K_{B,A} = g(\phi(\exp(y_A; x_B) \pmod{p_1}), \exp(v_A; s_B) \pmod{p_2}))$,

にて計算する。ただし、 g はハッシュ計算器内で用いられるハッシュ関数を表わし、 ϕ は、

【0091】

【数95】

【0092】 このとき、明らかに、 $K_{A,B} = K_{B,A}$ が成立する。

50 【0093】 さらに、A は電子メールを送信する機会が

多い利用者については、それらの利用者とAとの間の各マスタ鍵の集合 S_A 、または、Aの秘密情報 x_A から利用者側装置100A内の鍵生成器103Aにより鍵 $K(A)$ を作成し、暗復号化装置105Aを用いて鍵 $K(A)$ により S_A を暗号化した $C(A) = E(K(A); S_A)$ を、メモリ107Aに記憶する。以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに自分の秘密鍵と相手の公開鍵からマスタ鍵を作成することなく、メモリ107Aに記憶されているマスタ鍵を使う。

【0094】 メール本文の暗号化

Aは、利用者側装置100A内の乱数発生器101Aを用いて乱数 r を選び、 r を入力として鍵生成器103Aからデータ暗号化鍵 k を作成する。メール本文 P を暗復号化装置105Aを用いてデータ暗号化鍵 k により暗号化した暗号文 C_1 を、 $C_1 = E(k; P)$ にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵 k をマスタ鍵 $K_{A,B}$ で暗号化した暗号文 C_2 を、 $C_2 = E(K_{A,B}; k)$ にて作成する。

【0095】 Aは、通信装置108Aを用いて C_1 と C_2 をBに送る。

【0096】 メール本文の復号化

Bは送られてきた C_1 と C_2 に対して、Bの利用者側装置100B内の暗復号化装置105Bを用いて、まず、マスタ鍵 $K_{B,A}$ より、 $k = D(K_{B,A}; C_2)$ にてデータ暗号化鍵 k を復号化し、次にデータ暗号化鍵 k を用いて、 $P = D(k; C_1)$ にて、メール本文 P を復号化する。

【0097】 (実施例3) 実施例3は、実施例2においてセンタが作成する利用者 λ のための情報(s_λ, v_λ)を実施例2とは異なる別の関数により作成する一例を与える。

【0098】 準備

センタはセンタ側装置200内の素数発生器201、原始根生成器202および演算器204を用いて次の情報を作成する。ただし、関数 f は秘密鍵作成装置203内に格納されているものとする。

【0099】 公開情報:

- ・ p_1 ; 素数,
- ・ $p_2 = 2q_1q_2 + 1$; 素数,
- ・ $a_1 \in \mathbb{Z} \text{ s.t. } 0 < a_1 < p_1$, かつ, a_1 は $\mathbb{Z}/(p_1)$ で原始根,
- ・ $a_2 \in \mathbb{Z} \text{ s.t. } 0 < a_2 < p_2$, かつ, a_1 は $\mathbb{Z}/(p_1)$ で原始根,

秘密情報:

- ・ $q_1, q_2 \in \mathbb{Z}$; 素数.
- ネットワークの各利用者 λ は利用者側装置100内の乱数発生器101およびべき乗算器102を用いて次の鍵を作成する。

【0100】 秘密鍵:

【0101】

【数96】 $\cdot x_\lambda \in \mathbb{Z} \text{ s.t. } 0 < x_\lambda < p_1 - 1$.

公開鍵:

【0102】

【数97】 $\cdot y_\lambda = \exp(a_1; x_\lambda) \pmod{p_1}$.

センタへの登録

ネットワークの利用者 λ はセンタに自分のID情報 I_λ を登録する。

【0103】 センタはセンタ側装置200内の秘密鍵作成装置203を用いて、利用者 λ のID情報 I_λ に対して、

- (1) $I_\lambda + i_\lambda \pmod{p_2 - 1}$ は平方剰余,
- (2) $I_\lambda + i_\lambda \pmod{p_2 - 1} \neq I_\mu + i_\mu \pmod{p_2 - 1} \text{ if } \lambda \neq \mu$,

となるように正整数 i_λ を選び、

【0104】

【数98】

$s_\lambda = \exp(I_\lambda + i_\lambda; 1/2) \pmod{p_2 - 1}$ を計算して、 s_λ を利用者 λ に安全に配布する。

【0105】 このとき、明らかに、 $s_\lambda \neq s_\mu \text{ if } \lambda \neq \mu$, が成立する。

20 【0106】 マスタ鍵の共有

ネットワークの利用者 λ は、ベクトル(y_λ, v_λ)を λ の公開鍵として登録を行なう。ただし、 $v_\lambda = \exp(a_2; s_\lambda) \pmod{p_2}$ 。さらに、ネットワークに接続された利用者側装置100内には同一の秘密鍵暗号系アルゴリズムを内蔵した暗復号化装置105があり、この秘密鍵暗号系アルゴリズムを用いて平文 M を鍵 K で暗号化した結果および復号化した結果をそれぞれ $E(K; M)$, $D(K; M)$ で表わす。

【0107】 ネットワークの利用者A, Bについて、AはBに対して電子メールを送りたい。この目的の下で、A, Bは次の手順を実行する

AはAの利用者側装置100A内のべき乗算器102Aと演算器104Aとハッシュ計算器106Aを用いて、Aの秘密鍵

(x_A, s_A)とBの公開鍵(y_B, v_B)からマスタ鍵 $K_{A,B}$ を、

【0108】

【数99】 $K_{A,B} = g(\phi(\exp(y_B; x_A) \pmod{p_1}), \exp(v_B; s_A) \pmod{p_2}))$,

にて作成する。同様に、BはBの利用者側装置100B内のべき乗算器102Bと演算器104Bとハッシュ計算器106Bを用いて、Bの秘密鍵(x_B, s_B)とAの公開鍵(y_A, v_A)からマスタ鍵 $K_{B,A}$ を、

【0109】

【数100】 $K_{B,A} = g(\phi(\exp(y_A; x_B) \pmod{p_1}), \exp(v_A; s_B) \pmod{p_2}))$,

にて計算する。ただし、 g はハッシュ計算器内で用いられるハッシュ関数を表わし、 ϕ は、

【0110】

【数101】

$$\phi: Z/(p_1) \times Z/(p_2) \rightarrow Z/(n) \quad ((x, x) \rightarrow x),$$

なる同型写像を表わす ($n = p_1 p_2$)。ここで、 x はそれぞれの剰余環における x を代表元とする剰余類を表わす。

【0111】このとき、明らかに、 $K_{A,B} = K_{B,A}$ が成立する。

【0112】さらに、 A は電子メールを送信する機会が多い利用者については、それらの利用者と A との間の各マスタ鍵の集合 S_A 、または、 A の秘密情報 x_A から利用者側装置100A内の鍵生成器103Aにより鍵 $K(A)$ を作成し、暗復号化装置105Aを用いて鍵 $K(A)$ により S_A を暗号化した $C(A) = E(K(A); S_A)$ を、メモリ107Aに記憶する。以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに自分の秘密鍵と相手の公開鍵からマスタ鍵を作成することなく、メモリ107Aに記憶されているマスタ鍵を使う。

【0113】メール本文の暗号化

A は、利用者側装置100A内の乱数発生器101Aを用いて乱数 r を選び、 r を入力として鍵生成器103Aからデータ暗号化鍵 k を作成する。メール本文 P を暗復号化装置105Aを用いてデータ暗号化鍵 k により暗号化した暗号文 C_1 を、 $C_1 = E(k; P)$ にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵 k をマスタ鍵 $K_{A,B}$ で暗号化した暗号文 C_2 を、 $C_2 = E(K_{A,B}; k)$ にて作成する。

【0114】 A は、通信装置108Aを用いて C_1 と C_2 を B に送る。

【0115】メール本文の復号化

B は送られてきた C_1 と C_2 に対して、 B の利用者側装置100B内の暗復号化装置105Bを用いて、まず、マスタ鍵 $K_{B,A}$ より、 $k = D(K_{B,A}; C_2)$ にてデータ暗号化鍵 k を復号化し、次にデータ暗号化鍵 k を用いて、 $P = D(k; C_1)$ にて、メール本文 P を復号化する。

【0116】(実施例4) 実施例4は、実施例2、3においてセンタが作成する利用者 λ のための情報 (s_λ, v_λ) を実施例2、3とは異なる別の関数により作成する一例を与える。

【0117】準備

センタはセンタ側装置200内の素数発生器201、原始根生成器202および演算器204を用いて次の情報を作成する。

【0118】公開情報:

- ・ p_1 : 素数,
- ・ p_2 : 素数,
- ・ $a_1 \in Z$ s.t. $0 < a_1 < p_1$ 、かつ、 a_1 は $Z/(p_1)$ で原始根,
- ・ $a_2 \in Z$ s.t. $0 < a_2 < p_2$ 、かつ、 a_1 は $Z/(p_1)$ で原始根,
- 秘密情報:
- ・ $Z/(p_2 - 1)$ の元を出力する秘密鍵暗号アルゴリズム

μ および鍵 $r \in Z$ 。

センタの秘密情報である秘密鍵暗号アルゴリズムにより、平文 M を鍵 k で暗号化および復号化した結果をそれぞれ $E_0(k; M)$ 、 $D_0(k; M)$ で表わす。

【0119】ネットワークの各利用者 λ は利用者側装置100内の乱数発生器101およびべき乗算器102を用いて次の鍵を作成する。

【0120】秘密鍵:

【0121】

【数102】 $x_\lambda \in Z$ s.t. $0 < x_\lambda < p_1 - 1$ 。

公開鍵:

【0122】

【数103】 $y_\lambda = \exp(a_1; x_\lambda) \pmod{p_1}$ 。

センタへの登録

ネットワークの利用者 λ はセンタに自分のID情報 I_λ を登録する。

【0123】センタは、センタ側装置200内の秘密鍵作成装置203を用いて、利用者 λ のID情報 I_λ に対し

て、

【0124】

【数104】 $s_\lambda = E_0(r; I_\lambda) \in Z/(p_2 - 1)$ 、を計算して、 s_λ を利用者 λ に安全に配布する。

【0125】このとき、

【0126】

【数105】

$s_\lambda \neq s_\mu$ if $I_\lambda \neq I_\mu \in \Lambda = Z/(p_2 - 1)$ 、が成立することに注意する。

【0127】マスタ鍵の共有

ネットワークの利用者 λ は、ベクトル (y_λ, v_λ) を λ の公開鍵として登録を行なう。ただし、 $v_\lambda = \exp(a_2; s_\lambda) \pmod{p_2}$ 。さらに、ネットワークに接続された利用者側装置100内には同一の秘密鍵暗号系アルゴリズムを内蔵した暗復号化装置105があり、この秘密鍵暗号系アルゴリズムを用いて平文 M を鍵 K で暗号化した結果および復号化した結果をそれぞれ $E(K; M)$ 、 $D(K; M)$ で表わす。

【0128】ネットワークの利用者 A, B について、 A は B に対して電子メールを送りたい。この目的の下で、

A, B は次の手順を実行する

A は A の利用者側装置100A内のべき乗算器102Aと演算器104Aとハッシュ計算器106Aを用いて、 A の秘密鍵

(x_A, s_A) と B の公開鍵 (y_B, v_B) からマスタ鍵 $K_{A,B}$ を、

【0129】

【数106】 $K_{A,B} = g(\phi(\exp(y_B; x_A) \pmod{p_1}, \exp(v_B; s_A) \pmod{p_2}))$

にて作成する。同様に、 B は B の利用者側装置100B内のべき乗算器102Bと演算器104Bとハッシュ計算器106Bを用いて、 B の秘密鍵 (x_B, s_B) と A の公開鍵 ($y_A,$

v_A) からマスタ鍵 $K_{B,A}$ を、

【0130】

【数107】 $K_{B,A} = g(\phi(\exp(y_A : x_B) \pmod{p_1}), \exp(v_A : s_B) \pmod{p_2}))$,

$$\phi : Z/(p_1) \times Z/(p_2) \rightarrow Z/(n) \quad ((x, x) \rightarrow x),$$

なる同型写像を表わす ($n = p_1 p_2$)。ここで、 x はそれぞれの剰余環における x を代表元とする剰余類を表わす。

【0132】このとき、明らかに、 $K_{A,B} = K_{B,A}$ が成立する。

【0133】さらに、 A は電子メールを送信する機会が多い利用者については、それらの利用者と A との間の各マスタ鍵の集合 S_A 、または、 A の秘密情報 x_A から利用者側装置100A内の鍵生成器103Aにより鍵 $K(A)$ を作成し、暗復号化装置105Aを用いて鍵 $K(A)$ により S_A を暗号化した $C(A) = E(K(A) : S_A)$ を、メモリ107Aに記憶する。以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに自分の秘密鍵と相手の公開鍵からマスタ鍵を作成することなく、メモリ107Aに記憶されているマスタ鍵を使う。

【0134】 メール本文の暗号化

A は、利用者側装置100A内の乱数発生器101Aを用いて乱数 r を選び、 r を入力として鍵生成器103Aからデータ暗号化鍵 k を作成する。メール本文 P を暗復号化装置105Aを用いてデータ暗号化鍵 k により暗号化した暗号文 C_1 を、 $C_1 = E(k : P)$ 、にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵 k をマスタ鍵 $K_{A,B}$ で暗号化した暗号文 C_2 を、 $C_2 = E(K_{A,B} : k)$ 、にて作成する。

【0135】 A は、通信装置108Aを用いて C_1 と C_2 を B に送る。

【0136】 メール本文の復号化

B は送られてきた C_1 と C_2 に対して、 B の利用者側装置100B内の暗復号化装置105Bを用いて、まず、マスタ鍵 $K_{B,A}$ より、 $k = D(K_{B,A} : C_2)$ 、にてデータ暗号化鍵 k を復号化し、次にデータ暗号化鍵 k を用いて、 $P = D(k : C_1)$ 、にて、メール本文 P を復号化する。

【0137】(実施例5) 実施例5は実施例2の拡張版であり、 α の値を秘密にすることで安全性をさらに向上させている。

【0138】 準備

センタはセンタ側装置200内の素数発生器201、原始根生成器202および演算器204を用いて次の情報を作成する。

【0139】公開情報：

- ・ p ; 素数,
 - ・ $n = q \cdot q'$,
 - ・ $a \in Z$ s.t. $0 < a < p$ 、かつ、 a は $Z/(p)$ で原始根,
- 秘密情報：

にて計算する。ただし、 g はハッシュ計算器内で用いられるハッシュ関数を表わし、 ϕ は、

【0131】

【数108】

- ・ $q, q' \in Z$; 素数 s.t. $q-1 = 2 \xi_1 \xi_2$, $q'-1 = 2 \eta_1 \eta_2$ ($\xi_1, \xi_2, \eta_1, \eta_2$; 素数),
- ・ $\alpha \in Z$ s.t. α は $Z/(q)$, $Z/(q')$ で原始根.

ネットワークの各利用者 λ は利用者側装置100内の乱数発生器101およびべき乗算器102を用いて次の鍵を作成する。

【0140】秘密鍵：

【0141】

【数109】 $x_\lambda \in Z$ s.t. $0 < x_\lambda < p-1$.

公開鍵：

【0142】

【数110】 $y_\lambda = \exp(a : x_\lambda) \pmod{p}$.

センタへの登録

ネットワークの利用者 λ はセンタに自分のID情報 I_λ を登録する。

【0143】センタはセンタ側装置200内の秘密鍵作成装置203を用いて、 $ed \equiv 1 \pmod{M}$ 、なる e, d を作成し、利用者 λ のID情報 I_λ に対して、 $s_\lambda = \exp(I_\lambda : e) \pmod{N}$ 、

【0144】

【数111】 $v_\lambda = \exp(\alpha : s_\lambda) \pmod{n}$ 、

を計算して、 (s_λ, v_λ) を利用者 λ に安全に配布する。ただし、 $M = \text{l.c.d}(\xi_1-1, \xi_2-1, \eta_1-1, \eta_2-1)$ 、 $N = \text{l.c.d}(q-1, q'-1)$ 。

30 【0145】このとき、

【0146】

【数112】 $s_\lambda \neq s_\mu$ and $v_\lambda \neq v_\mu$ if $I_\lambda \neq I_\mu$
 $\in \Lambda = Z/(N)$ 、

が成立することに注意する。

【0147】 マスタ鍵の共有

ネットワークの利用者 λ は、ベクトル (y_λ, v_λ) を λ の公開鍵として登録を行なう。

【0148】さらに、ネットワークに接続された利用者側装置100内には同一の秘密鍵暗号系アルゴリズムを内蔵した暗復号化装置105があり、この秘密鍵暗号系アルゴリズムを用いて平文 M を鍵 K で暗号化した結果および復号化した結果をそれぞれ $E(K : M)$ 、 $D(K : M)$ で表わす。

【0149】ネットワークの利用者 A, B について、 A は B に対して電子メールを送りたい。この目的の下で、 A, B は次の手順を実行する
 A は A の利用者側装置100A内のべき乗算器102Aと演算器104Aとハッシュ計算器106Aを用いて、 A の秘密鍵 (x_A, s_A) と B の公開鍵 (y_B, v_B) からマスタ鍵 K

50 A, B を、

【0150】

【数113】 $K_{A,B} = g(\phi(\exp(y_B : x_A) \pmod{p}), \exp(v_B : s_A) \pmod{n}))$,

にて作成する。同様に、BはBの利用者側装置100B内のべき乗算器102Bと演算器104Bとハッシュ計算器106Bを用いて、自分の秘密鍵 (x_B, s_B) とAの公開鍵 (y_A, v_A) からマスタ鍵 $K_{B,A}$ を、

$$\phi : Z/(p) \times Z/(n) \rightarrow Z/(m) \quad ((x, x) \rightarrow x),$$

なる同型写像を表わす ($m = pn$)。ここで、 x はそれぞれの剰余環における x を代表元とする剰余類を表わす。

【0153】このとき、明らかに、 $K_{A,B} = K_{B,A}$ が成立する。

【0154】さらに、Aは電子メールを送信する機会が多い利用者については、それらの利用者とAとの間の各マスタ鍵の集合 S_A 、または、Aの秘密情報 x_A から利用者側装置100A内の鍵生成器103Aにより鍵 $K(A)$ を作成し、暗復号化装置105Aを用いて鍵 $K(A)$ により S_A を暗号化した $C(A) = E(K(A); S_A)$ を、メモリ107Aに記憶する。以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに自分の秘密鍵と相手の公開鍵からマスタ鍵を作成することなく、メモリ107Aに記憶されているマスタ鍵を使う。

【0155】 メール本文の暗号化

Aは、利用者側装置100A内の乱数発生器101Aを用いて乱数 r を選び、 r を入力として鍵生成器103Aからデータ暗号化鍵 k を作成する。メール本文 P を暗復号化装置105Aを用いてデータ暗号化鍵 k により暗号化した暗号文 C_1 を、 $C_1 = E(k; P)$ 、にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵 k をマスタ鍵 $K_{A,B}$ で暗号化した暗号文 C_2 を、 $C_2 = E(K_{A,B}; k)$ 、にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵 k をマスタ鍵 $K_{A,B}$ で暗号化した暗号文 C_2 を、 $C_2 = E(K_{A,B}; k)$ 、にて作成する。

【0156】Aは、通信装置108Aを用いて C_1 と C_2 をBに送る。

【0157】 メール本文の復号化

Bは送られてきた C_1 と C_2 に対して、Bの利用者側装置100B内の暗復号化装置105Bを用いて、まず、マスタ鍵 $K_{B,A}$ より、 $k = D(K_{B,A}; C_2)$ 、にてデータ暗号化鍵 k を復号化し、次にデータ暗号化鍵 k を用いて、 $P = D(k; C_1)$ 、にて、メール本文 P を復号化する。

【0158】(実施例6) 実施例6は実施例3の拡張版であり、 α の値を秘密にすることにより安全性をさらに向上させている。

【0159】 準備

センタはセンタ側装置200内の素数発生器201、原始根生成器202および演算器204を用いて次の情報を作成する。ただし、関数 f は秘密鍵作成装置203内に格納されてい

【0151】

【数114】 $K_{B,A} = g(\phi(\exp(y_A : x_B) \pmod{p}), \exp(v_A : s_B) \pmod{n}))$,

にて計算する。ただし、 g はハッシュ計算器内で用いられるハッシュ関数を表わし、 ϕ は、

【0152】

【数115】

$((x, x) \rightarrow x)$ 、
るものとする。

【0160】 公開情報：

- ・ p ; 素数,
- ・ $n = q \cdot q'$,
- ・ $a \in Z$ s.t $0 < a < p$ 、かつ、 a は $Z/(p)$ で原始根,

秘密情報：

- ・ $q, q' \in Z$; 素数 s.t $q-1 = 2^{\xi_1} \xi_2$, $q'-1 = 2^{\eta_1} \eta_2$ ($\xi_1, \xi_2, \eta_1, \eta_2$; 素数),
- ・ $\alpha \in Z$ s.t α は $Z/(q)$, $Z/(q')$ で原始根.
- ・ f ; 擬似ランダム関数.

20 ネットワークの各利用者 λ は利用者側装置100内の乱数発生器101およびべき乗算器102を用いて次の鍵を作成する。

【0161】 秘密鍵：

【0162】

【数116】 $x_\lambda \in Z$ s.t $0 < x_\lambda < p-1$.

公開鍵：

【0163】

【数117】 $y_\lambda = \exp(a : x_\lambda) \pmod{p}$.

センタへの登録

30 ネットワークの利用者 λ はセンタに自分のID情報 I_λ を登録する。

【0164】センタはセンタ側装置200内の秘密鍵作成装置203を用いて、利用者 λ のID情報 I_λ に対して、

(1) $I_\lambda + i_\lambda \pmod{N}$ は平方剰余、
(2) $I_\lambda + i_\lambda \pmod{N} \neq I_\mu + i_\mu \pmod{N}$

if $\lambda \neq \mu$ 、

となるように正整数 i_λ を選び、

【0165】

【数118】 $s_\lambda = \exp(I_\lambda + i_\lambda : 1/2) \pmod{N}$,

40 $v_\lambda = \exp(\alpha : s_\lambda) \pmod{n}$,

を計算して、 (s_λ, v_λ) を利用者 λ に安全に配布する。

【0166】このとき、明らかに、 $s_\lambda \neq s_\mu$, $v_\lambda \neq v_\mu$ if $\lambda \neq \mu$ 、が成立する。

【0167】 マスタ鍵の共有

ネットワークの利用者 λ は、ベクトル (y_λ, v_λ) を λ の公開鍵として登録を行なう。

【0168】さらに、ネットワークに接続された利用者側装置100内には同一の秘密鍵暗号系アルゴリズムを内蔵した暗復号化装置105があり、この秘密鍵暗号系アル

ゴリズムを用いて平文Mを鍵Kで暗号化した結果および復号化した結果をそれぞれE(K;M), D(K;M)で表わす。

【0169】ネットワークの利用者A, Bについて、AはBに対して電子メールを送りたい。この目的の下で、A, Bは次の手順を実行する

AはAの利用者側装置100A内のべき乗算器102Aと演算器104Aとハッシュ計算器106Aを用いて、Aの秘密鍵

(x_A, s_A)とBの公開鍵(y_B, v_B)からマスタ鍵 $K_{A,B}$ を、

【0170】

【数119】 $K_{A,B} = g(\phi(\exp(y_B : x_A) \pmod{p}), \exp$

$$\phi : Z/(p) \times Z/(n) \rightarrow Z/(m) \quad ((x, x) \rightarrow x),$$

なる同型写像を表わす($m=pn$)。ここで、 x はそれぞれの剰余環における x を代表元とする剰余類を表わす。

【0173】このとき、明らかに、 $K_{A,B}=K_{B,A}$ が成立する。

【0174】さらに、Aは電子メールを送信する機会が多い利用者については、それらの利用者とAとの間の各マスタ鍵の集合 S_A 、または、Aの秘密情報 x_A から利用者側装置100A内の鍵生成器103Aにより鍵K(A)を作成し、暗復号化装置105Aを用いて鍵K(A)により S_A を暗号化した $C(A)=E(K(A); S_A)$ を、メモリ107Aに記憶する。以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに自分の秘密鍵と相手の公開鍵からマスタ鍵を作成することなく、メモリ107Aに記憶されているマスタ鍵を使う。

【0175】メール本文の暗号化

Aは、利用者側装置100A内の乱数発生器101Aを用いて乱数 r を選び、 r を入力として鍵生成器103Aからデータ暗号化鍵 k を作成する。メール本文 P を暗復号化装置105Aを用いてデータ暗号化鍵 k により暗号化した暗号文 C_1 を、 $C_1=E(k; P)$ にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵 k をマスタ鍵 $K_{A,B}$ で暗号化した暗号文 C_2 を、 $C_2=E(K_{A,B}; k)$ にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵 k をマスタ鍵 $K_{A,B}$ で暗号化した暗号文 C_2 を、 $C_2=E(K_{A,B}; k)$ にて作成する。

【0176】Aは、通信装置108Aを用いて C_1 と C_2 をBに送る。

【0177】メール本文の復号化

Bは送られてきた C_1 と C_2 に対して、Bの利用者側装置100B内の暗復号化装置105Bを用いて、まず、マスタ鍵 $K_{B,A}$ より、 $k=D(K_{B,A}; C_2)$ にてデータ暗号化鍵 k を復号化し、次にデータ暗号化鍵 k を用いて、 $P=D(k; C_1)$ にて、メール本文 P を復号化する。

【0178】(実施例7) 実施例7は実施例4の拡張版であり、 α の値を秘密にすることにより安全性をさらに

($v_B : s_A \pmod{n}$))、

にて作成する。同様に、BはBの利用者側装置100B内のべき乗算器102Bと演算器104Bとハッシュ計算器106Bを用いて、自分の秘密鍵(x_B, s_B)とAの公開鍵(y_A, v_A)からマスタ鍵 $K_{B,A}$ を、

【0171】

【数120】 $K_{B,A} = g(\phi(\exp(y_A : x_B) \pmod{p}), \exp$

($v_A : s_B \pmod{n}$))、

10 にて計算する。ただし、 g はハッシュ計算器内で用いられるハッシュ関数を表わし、 ϕ は、

【0172】

【数121】

向上させている。

【0179】準備

センタはセンタ側装置200内の素数発生器201、原始根生成器202および演算器204を用いて次の情報を作成する。

【0180】公開情報：

- ・ p ；素数、
- 20 20 $\cdot n = q \cdot q'$ (q, q' ；素数)，
- ・ $a \in Z$ s.t $0 < a < p$ 、かつ、 a は $Z/(p)$ で原始根、

秘密情報：

- ・ $Z/(N)$ の元を出力する秘密鍵暗号アルゴリズムおよび鍵 r 、
- ・ $\alpha \in Z$ s.t α は $Z/(q)$ 、 $Z/(q')$ で原始根。

ここで、 $N=1.c.d(q-1, q'-1)$ とする。また、センタの秘密情報である秘密鍵暗号アルゴリズムにより、平文Mを鍵 k で暗号化および復号化した結果をそれぞれ $E_0(k; M)$ 、 $D_0(k; M)$ で表わす。

【0181】ネットワークの各利用者 λ は利用者側装置100内の乱数発生器101およびべき乗算器102を用いて次の鍵を作成する。

【0182】秘密鍵：

【0183】

【数122】 $\cdot x_\lambda \in Z$ s.t $0 < x_\lambda < p-1$ 。

公開鍵：

【0184】

【数123】 $\cdot y_\lambda = \exp(a : x_\lambda) \pmod{p}$ 。

40 センタへの登録

ネットワークの利用者 λ はセンタに自分のID情報 I_λ を登録する。

【0185】センタはセンタ側装置200内の秘密鍵作成装置203を用いて、利用者 λ のID情報 I_λ に対して、

【0186】

【数124】 $s_\lambda = E_0(r; I_\lambda) \in Z/(N)$ 、

$v_\lambda = \exp(\alpha : s_\lambda) \pmod{N}$ 、

を計算して、(s_λ, v_λ)を利用者 λ に安全に配布する。

50 【0187】このとき、 $s_\lambda \neq s_\mu$ and $v_\lambda \neq v_\mu$ i

$f \mid \lambda \neq \mu \in \Lambda = Z/(N)$, が成立することに注意する。

【0188】 マスタ鍵の共有

ネットワークの利用者 λ は、ベクトル (y_λ, v_λ) を λ の公開鍵として登録を行なう。

【0189】さらに、ネットワークに接続された利用者側装置100内には同一の秘密鍵暗号系アルゴリズムを内蔵した暗復号化装置105があり、この秘密鍵暗号系アルゴリズムを用いて平文 M を鍵 K で暗号化した結果および復号化した結果をそれぞれ $E(K; M)$, $D(K; M)$ で表わす。

【0190】ネットワークの利用者 A, B について、 A は B に対して電子メールを送りたい。この目的の下で、 A, B は次の手順を実行する
 A は A の利用者側装置100A内のべき乗算器102Aと演算器104Aとハッシュ計算器106Aを用いて、 A の秘密鍵

$$\phi: Z/(p) \times Z/(n) \rightarrow Z/(m) \quad ((x, x) \rightarrow x),$$

なる同型写像を表わす($m=pn$)。ここで、 x はそれぞれの剰余環における x を代表元とする剰余類を表わす。

【0194】このとき、明らかに、 $K_{A,B}=K_{B,A}$, が成立する。

【0195】さらに、 A は電子メールを送信する機会が多い利用者については、それらの利用者と A との間の各マスタ鍵の集合 S_A 、または、 A の秘密情報 x_A から利用者側装置100A内の鍵生成器103Aにより鍵 $K(A)$ を作成し、暗復号化装置105Aを用いて鍵 $K(A)$ により S_A を暗号化した $C(A)=E(K(A); S_A)$, を、メモリ107Aに記憶する。以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに自分の秘密鍵と相手の公開鍵からマスタ鍵を作成することなく、メモリ107Aに記憶されているマスタ鍵を使う。

【0196】 メール本文の暗号化

A は、利用者側装置100A内の乱数発生器101Aを用いて乱数 r を選び、 r を入力として鍵生成器103Aからデータ暗号化鍵 k を作成する。メール本文 P を暗復号化装置105Aを用いてデータ暗号化鍵 k により暗号化した暗号文 C_1 を、 $C_1=E(k; P)$, にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵 k をマスタ鍵 $K_{A,B}$ で暗号化した暗号文 C_2 を、 $C_2=E(K_{A,B}; k)$, にて作成する。

【0197】 A は、通信装置108Aを用いて C_1 と C_2 を B に送る。

【0198】 メール本文の復号化

B は送られてきた C_1 と C_2 に対して、 B の利用者側装置100B内の暗復号化装置105Bを用いて、まず、マスタ鍵 $K_{B,A}$ より、 $k=D(K_{B,A}; C_2)$, にてデータ暗号化鍵 k を復号化し、次にデータ暗号化鍵 k を用いて、 $P=D(k; C_1)$, にて、メール本文 P を復号化する。

(x_A, s_A) と B の公開鍵 (y_B, v_B) からマスタ鍵 $K_{A,B}$ を、

【0191】

【数125】 $K_{A,B}=g(\phi(\exp(y_B; x_A) \pmod{p}), \exp(v_B; s_A) \pmod{n}))$,

にて作成する。同様に、 B は B の利用者側装置100B内のべき乗算器102Bと演算器104Bとハッシュ計算器106Bを用いて、自分の秘密鍵 (x_B, s_B) と A の公開鍵 (y_A, v_A) からマスタ鍵 $K_{B,A}$ を、

10 【0192】

【数126】 $K_{B,A}=g(\phi(\exp(y_A; x_B) \pmod{p}), \exp(v_A; s_B) \pmod{n}))$,

にて計算する。ただし、 g はハッシュ計算器内で用いられるハッシュ関数を表わし、 ϕ は、

【0193】

【数127】

【0199】(実施例8) 実施例1から実施例7において、以下のようにメール本文の暗号化およびメール本文の復号化を行なう。

20

【0200】 ・メール本文の暗号化

A は、利用者側装置100A内の乱数発生器101Aを用いて乱数 r を選び、 r を入力として鍵生成器103Aからデータ暗号化鍵 k を作成する。メール本文 P を暗復号化装置105Aを用いてデータ暗号化鍵 k により暗号化した暗号文 C_1 を、 $C_1=E(k; P)$, にて作成する。さらに、演算器を用いてデータ暗号化鍵 k とマスタ鍵 $K_{A,B}$ の排他的論理和を、 $C_2=k * K_{A,B}$, にて作成する。

【0201】 A は通信装置108Aを用いて C_1 と C_2 を B に送る。

30

【0202】 ・メール本文の復号化

B は送られてきた C_1 と C_2 に対して、まず、演算器104Bを用いてマスタ鍵 $K_{B,A}$ と C_2 の排他的論理和を計算することによりデータ暗号化鍵 k を復号化する。すなわち、 $k=C_2 * K_{A,B}$, 次に、暗復号化装置105Bを用いてデータ暗号化鍵 k から、 $P=D(k; C_1)$, にてメール本文 P を復号化する。

【0203】(実施例9) 実施例2から実施例8のマスタ鍵共有において、 A は A の利用者側装置100A内のべき乗算器102Aと演算器104Aとハッシュ計算器106Aを用いて、 A の秘密鍵 (x_A, s_A) と B の公開鍵 (y_B, v_B) からマスタ鍵 $K_{A,B}$ を、

【0204】

【数128】 $K_{A,B}=g((\exp(y_B; x_A) \pmod{p}) * (\exp(v_B; s_A) \pmod{n}))$,

にて作成する。同様に、 B は B の利用者側装置100B内のべき乗算器102Bと演算器104Bとハッシュ計算器106Bを用いて、自分の秘密鍵 (x_B, s_B) と A の公開鍵 (y_A, v_A) からマスタ鍵 $K_{B,A}$ を、

50 【0205】

【数129】 $K_{B,A} = g \left(\left(\exp(y_A : x_B) \pmod{p} \right) * \left(\exp(v_A : s_B) \pmod{n} \right) \right)$,
にて計算する。ただし、 g はハッシュ計算器内で用いられるハッシュ関数を表わし、 $x * y$ は x と y の排他的論理和を表わす。

【0206】（実施例10）ネットワークの各利用者はカード400を所持し、電子メール通信時にはカード400を利用者側装置500内のカード読取装置501に差し込み、実施例1から実施例9において、利用者側装置100内の乱数発生器101、べき乗算器102、鍵生成器103、演算器104、暗復号化装置105、ハッシュ計算器106、メモリ107を用いて行なう処理をそれぞれカード400内の乱数発生器401、べき乗算器402、鍵生成器403、演算器404、暗復号化装置405、ハッシュ計算器406、メモリ407を用いて行ない、受信者への送信文はカード400内の出力装置408を用いて、利用者側装置500内のカード読取装置501に出力され、さらに、利用者側装置500内の通信装置502を用いて通信回線300を介して送信する。

【0207】

【発明の効果】本発明における電子メール暗号化方法によれば、メールシステムや機種に特定しないで通常のメールと併用できる特徴を有するため、通信ネットワークの形態に依らず適用が可能である。また、電子メールの送信者および受信者はそれぞれ自分の秘密鍵と相手の公開鍵からマスタ鍵の共有を行ない、秘密鍵暗号を用いてメール本文の暗号化およびデータ暗号化鍵配送を行なっているため、送受信者双方の計算処理負担が少なく高速な暗号化処理が可能となった。また、デジタル署名などの付加情報を付けることなく送信者の認証が可能となるため、メール暗号文のヘッダ情報が少なく、電子メー

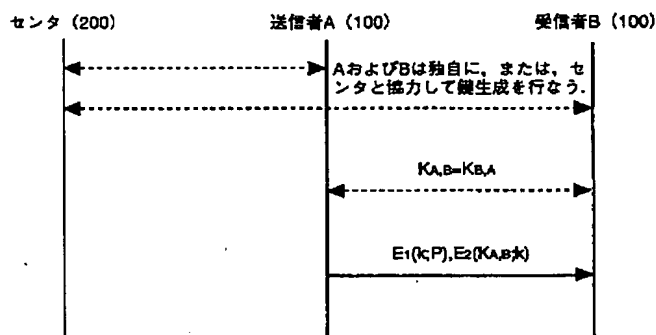
10

20

30

【図2】

図 2



ルのセキュリティ機能実現のための処理時間が大幅に削減された。さらに、ID情報は利用者毎に異なることを利用して、センタと利用者が協力して利用者の鍵生成を行なうことにより、利用者の鍵の一致の心配がなく、盗聴や不正者のなりすまし対して高い安全性を実現した。

【図面の簡単な説明】

【図1】本発明の実施例におけるシステム構成を示すブロック図。

【図2】本発明の電子メール暗号化方法の概念を示す説明図。

【図3】実施例1から9のシステム構成内の利用者側装置内部構成を示すブロック図。

【図4】実施例1から9のシステム構成内のセンタ側装置内部構成を示すブロック図。

【図5】実施例10のシステム構成内のカード内部構成を示すブロック図。

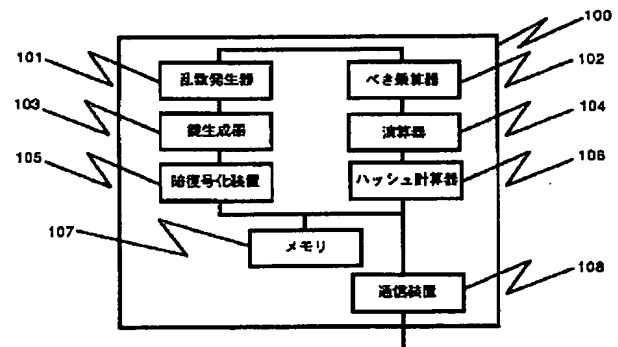
【図6】実施例10のシステム構成内の利用者側装置内部構成を示すブロック図。

【符号の説明】

- 100…利用者側装置、
- 101…利用者側装置100内の乱数発生器、
- 102…利用者側装置100内のべき乗算器、
- 103…利用者側装置100内の鍵生成器、
- 104…利用者側装置100内の演算器、
- 105…利用者側装置100内の暗復号化装置、
- 106…利用者側装置100内のハッシュ計算器、
- 107…利用者側装置100内のメモリ、
- 108…利用者側装置100内の通信装置、
- 200…センタ側装置。

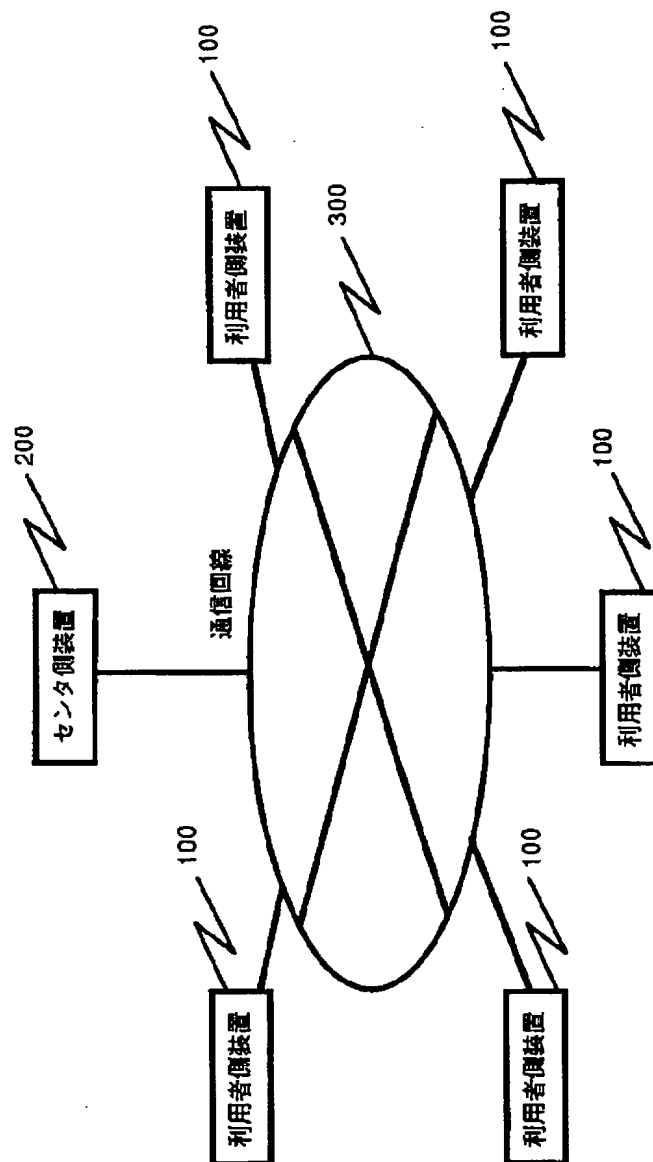
【図3】

図 3



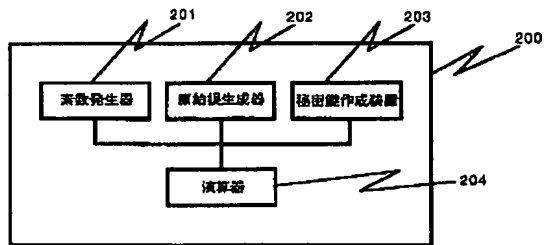
【図 1】

図 1



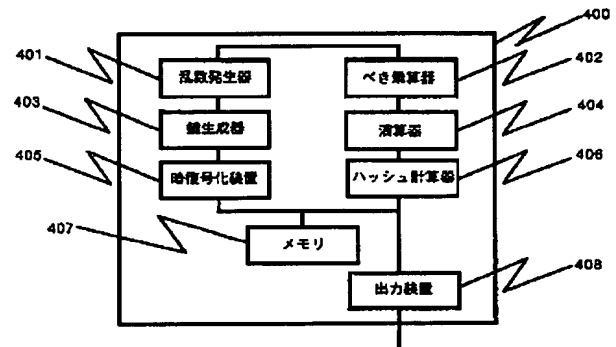
【図 4】

図 4



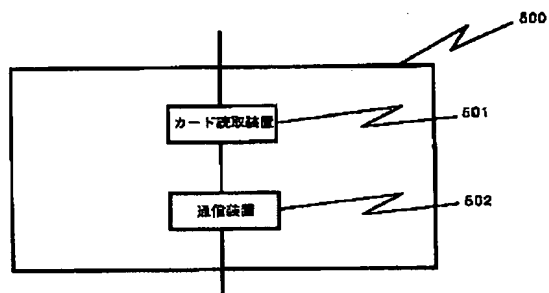
【図 5】

図 5



【図 6】

図 6



フロントページの続き

(51) Int. Cl. ⁶

H 0 4 L 12/58

識別記号

庁内整理番号

F I

技術表示箇所